



APPLICANT PRIVACY NOTICE

Introduction / Scope of Notice

This privacy notice applies to all applicants for employment (whether permanent or temporary) with ESO. This notice sets out the basis upon which we collect, use, store, share and keep secure the personal information provided to us in connection with your application.

As the controller of the information, ESO is responsible for deciding how we hold and use personal information about you. You are being provided a copy of this notice because you are applying for work with us (whether as an employee, intern, or contractor).

This notice makes you aware of how and why we collect and process personal information for recruitment purposes. It provides you with certain information about rights which you may have under the General Data Protection Regulation (GDPR – both the EU and UK versions), the Personal Information Protection and Electronic Documents Act (PIPEDA) or the California Consumer Protection Act (CCPA) (this is not an exhaustive list).

This notice also sets out details of how to contact ESO if you have any questions or comments, or if you would like to exercise any of your rights with respect to personal information about you.

Table of Contents

Introduction / Scope of Notice	1
Glossary / Terms used	2
Your Personal Information	2
Purpose and Legal Basis for Processing	2
Special Categories of Personal Information	3
Personal Information Relating to Crimes	4
Disclosure of Your Personal Information	4
Transfer of Personal Information outside the EEA.....	5
Data Privacy Framework	5
Security of Your Personal Information	6
Retention of Personal Information	6
Your Rights	7
Complaints	10
How to contact us	10

Glossary / Terms used.

Term	Meaning
Data subject	A data subject is someone who can be identified from personal data or personal information. In the context of this notice, users may be data subjects.
Data Controller or Controller	A data controller is usually a company, who will have the responsibility of deciding how personal data is processed and protected from harm.
Data Processor or processor	A data processor will process data on behalf of a controller. They will follow the instructions of the controller while protecting the data from harm. A data processor does not own data.
Personal Data / Personal Information	Personal data is information about who you are, where you live, what you do and more. In the context of this notice, personal data will be data that is provided either via technology or by contacting the website owner (ESO Solutions, Inc) with feedback or a query etc. For the purposes of this notice, personal data and personal information have the same meaning.

Your Personal Information

'Personal Data' is defined as any data relating to a living individual who can be identified directly from that data or indirectly in conjunction with other information. This is also called personal information and will be referred to as such throughout the remainder of the document.

As part of your application, we may collect the following information from you, (If you do not provide information that is necessary for us to consider your application, such as work history or qualifications, we may not be able to process your application or suitability for a particular role):

- Contact/identifying details including name, address, email address, contact phone numbers, date of birth, photo, civil status, emergency contact details.
- Curriculum Vitae and/or application form, previous employment background, references from previous employers, educational details, professional and/or academic transcripts.
- CCTV images captured through the legitimate use of CCTV within our offices; and

Purpose and Legal Basis for Processing

We will hold, process and may disclose personal information provided by you for the following purposes.

<ul style="list-style-type: none"> • Recruitment/appointment including assessing your job application. 	This use of your personal information is necessary to process job applications submitted by, or on your behalf, and for
---	---

<ul style="list-style-type: none"> • Provide you with building and IT access. 	<p>performance of your contract of employment.</p>
<ul style="list-style-type: none"> • Monitoring and promotion of equal opportunities, including the review of community background, gender breakdown and progression. • Provide references. • Investigate and respond to queries from unsuccessful applicants; and • Maintain emergency contact details. 	<p>This use of your personal information is necessary for our legitimate business interest in managing our business including legal, personnel, administrative and management purposes and for the prevention and detection of crime provided our interest are not overridden by your interest. Please note that you have a right to object to processing of your personal information where that processing is carried on for our legitimate interest.</p>
<ul style="list-style-type: none"> • Manage health and safety at work and report on incidents. • Comply with requirements of our lenders or grant making bodies (e.g., Invest Northern Ireland). • Monitoring community background and gender breakdown of your employees, applicants, appointees and, in some instances, promotes and leavers for the purpose of completing annual monitoring returns and Article 55 Revises as required by the Equality Commission for Northern Ireland; and • Exercising our right to defend, respond or conduct legal proceedings. 	<p>This use of your information is necessary in order for us to comply with any legal or regulatory obligations.</p>

We may, from time to time, (i) ask for you consent to use your personal information for a specific purpose; and/or (ii) process your personal information (including "special information") in order to protect your vital interests or the interests of another.

Special Categories of Personal Information

Certain categories of your personal information are regarded as 'special'. Special information includes information relating to an individual's:

- Physical or mental health.
- Religious and philosophical beliefs.
- Ethnic or racial origin.

- Biometric or genetic data; and
- Sex life and sexual orientation

We only process such information where necessary for:

- the purpose of carrying out the obligations, and exercising specific rights, of ESO or of a job applicant under employment law.
- the assessment of your working capacity; and/or
- the establishment, exercise, or defence of legal claims

If we wish to process your special personal information for any further purpose, we will seek your explicit consent to do so. You have the right to withdraw your consent to that processing at any time.

Personal Information Relating to Crimes

We will only process information relating to your criminal convictions or involvement in criminal proceedings when permitted or required by law, or where provided voluntarily by you.

Disclosure of Your Personal Information

We may disclose your personal information to members of our corporate group including, without limitation, for the following reasons: in order to run global processes, carry out group wide reporting, or take decisions about hiring or promotion.

It may be necessary from time to time for us to disclose your personal information to third parties or agents, including without limitation to the following:

- Third parties or agents of clients to assist in the administration, processing and management of certain activities pertaining to past, current and prospective employees.
- Individuals or companies employed by us to carry out specific services, functions or consultancy work including external reference agencies, email monitoring, provision of services related to employee and family securities accounts and other financial institutions.
- Relatives or legal representatives of past, current and prospective employees.
- Regulatory bodies to whom we are obliged or required to disclose information including the Office of the Industrial Tribunals and Fair Employment Tribunal, the Equality Commission for Northern Ireland, courts, and court-appointed persons.
- Legal and medical practitioners and occupational health specialists.
- Relevant Government departments and agencies; and
- Other support service providers necessary to support the organisation in the services listed.

We will inform you in advance if we intend to further process or disclose your personal information for a purpose other than the purposes set out in this Privacy Notice. We take all reasonable steps, as required by law, to ensure the safety, privacy and integrity of such information and enter into any required contracts with such third parties to protect the privacy and integrity of such information and any information supplied.

We may also disclose your personal information to our private equity sponsor, Vista Equity Partners, and its affiliates, including Vista Consulting Group (collectively "Vista"), for administration, research, database development, workforce analytics and business operation purposes, in line with the terms of this privacy notice. Vista processes and shares your personal information with its affiliates, including other Vista portfolio companies, on the basis of its legitimate interests in managing, administering, and improving its business and overseeing the recruitment process and, if applicable, your employment relationship with ESO Solutions. If you have consented to us doing so, we also share your personal information with other Vista portfolio companies for the purpose of being considered for other job opportunities in the pooling system, both inside and outside the EEA. Please find a full list of all Vista portfolio companies at <https://www.vistaequitypartners.com/companies/> and Vista's privacy policy at <https://www.vistaequitypartners.com/privacy/>. Where this requires us to transfer your personal information outside of the EEA, please refer to the privacy notice for further details on cross-border transfers. In connection with the recruitment process, your personal data may be transferred outside of the EEA to Lever, Hirebridge, LLC and Criteria Corp, which provide applicant tracking and evaluation services. Hirebridge, LLC and Criteria Corp have agreed to comply with the EU transfer mechanisms to ensure that your personal information is adequately protected whilst outside of the EEA.

Transfer of Personal Information outside the EEA

The personal information that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ('EEA'), for the purposes described above. Those countries may not provide an adequate level of protection in relation to processing your personal information. Due to the global nature of our business, your personal information may be disclosed to members of our group outside the EEA, including in particular in the USA. It may also be processed by personnel operating outside the EEA who work for us or for one of our suppliers who act on our behalf. We will ensure appropriate safeguards are in place to protect the privacy and integrity of such personal information.

Data Privacy Framework

ESO complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. ESO has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK

Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit [Data privacy framework website](#).

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, ESO commits to refer unresolved complaints concerning our handling of human resources personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. to either the EU Data Protection Authorities or the UK Information Commission. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit either [EU Data Protection Authorities \(DPAs\)](#) or [UK Information Commissioner's Office \(ICO\)](#).

The Federal Trade Commission has jurisdiction over ESO's compliance with the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. DPF.

Additionally, an individual has the possibility, under certain conditions, to invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms; for additional information: <https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2>

If ESO receives personal information under the DPF Principles and then transfers that personal information to a third-party, ESO shall remain liable under the DPF Principles to the extent the third party's actions are inconsistent with the DPF Principles, unless ESO provides information in support of ESO not having responsibility for the event.

Security of Your Personal Information

ESO is dedicated to safeguarding your personal information. We employ a range of industry-standard security technologies and procedures to protect your data from unauthorized access, use, or disclosure. While no method of transmission over the Internet or electronic storage is completely secure, we continuously strive to enhance our security measures. Despite our best efforts, we cannot guarantee absolute security, but we remain committed to protecting your personal information to the fullest extent possible.

Retention of Personal Information

Personal information of applicants who are not hired will be stored for 3 years and then destroyed in accordance with our legal obligations.

Personal information of applicants who are hired will be retained for the duration of employment and to the extent necessary to enable ESO to comply any legal obligations or for the exercise or defence of legal claims.

Your Privacy Rights in the UK, EEA, and Switzerland

If you reside in the UK, the EEA or Switzerland, you may have certain rights with respect to your personal information and the processing of it. The rights are outlined below:

- The right of access – Individuals may make a request to access their personal data / personal information.
- The right to be informed – Individuals have the right to be informed about the collection and usage of their personal data / personal information.
- The right of rectification – Individuals have the right to have any inaccurate or incomplete personal data / personal information rectified or updated as appropriate.
- The right to be forgotten (also called the right to erasure) – Individuals have the right to request that all personal data / personal information is deleted.
- The right to restrict processing of your data - Individuals have the right to request that processing of your personal data / personal information is restricted.
- The right to data portability - Individuals have the right to request that we have requested your permission to process your personal data / personal information, to receive that information you provided in a portable format.
- The right to object – Individuals have the right to object to the processing of their personal data / personal information.
- The right to object to automated processing – Individuals have the right to object to solely automated processing.

*Note – Individuals have these rights, but they may only be exercised in certain circumstances. Responses to any requests relating to the above rights will be free unless manifestly unfounded or excessive, in which case a reasonable fee may be applied.

To enable us to respond to your enquiry, we may need to request specific information from you to help us confirm your identity. This is a security measure to ensure that personal information is not shared with the incorrect individual. We may also ask you for further information where it will assist us in speeding up the response.

For requests about any of the above rights, please contact privacyoffice@eso.com.

Should you be unhappy with our response, you have the right to lodge a complaint with your local supervisory authority. In the UK, this is [Information Commissioner's Office \(ICO\)](#), if you are located in the EEA or Switzerland, you can find details of your local authority [here](#).

To submit a request to exercise any of the above rights, please contact privacyoffice@eso.com.

Your Privacy Rights in Canada

If you reside in Canada, you may have certain rights with respect to your personal information and the processing of it. The rights are outlined below:

- The right of access – Individuals may make a request to access their personal data / personal information.
- The right of rectification – Individuals have the right to have any inaccurate or incomplete personal information / personal data rectified or updated as appropriate.
- The right to withdraw your consent at any time.

*Note – Individuals have these rights, but they may only be exercised in certain circumstances.

To enable us to respond to your enquiry, we may need to request specific information from you to help us confirm your identity. This is a security measure to ensure that personal information is not shared with the incorrect individual. We may also ask you for further information where it will assist us in speeding up the response.

For requests about any of the above rights, please contact privacyoffice@eso.com.

Should you be unhappy with our response, you have the right to lodge a complaint with the Office of the Privacy Commissioner of Canada.

Your Privacy Rights in the USA

Several states across the USA have Privacy Acts which may provide rights to individuals who reside in those states. As there is no federal law, each state may offer different rights to individuals. This situation is constantly evolving and this notice will be reviewed regularly and updated when required, but here are some examples of laws that are already in place and the consumer rights that they provide:

USA Privacy Laws as at December 2024	Consumer Rights								
<u>Law Name</u>	Right to access	Right to correct	Right to delete	Right to opt out of certain processing	Right to portability	Right to opt out of sales	Right to opt in for sensitive data processing	Right against automated decision making	Private right of action
California Consumer Privacy Act 2018, amended by the California Privacy Rights Act 2020.	X	X	X	S	X	X		X	L
Colorado Privacy Act 2023	X	X	X	P	X	X	X	X~	
Connecticut Data Privacy Act 2023	X	X	X	P	X	X	X	X~	

Montana Consumer Data Privacy Act 2024	X	X	X	P	X	X	X	X~	
Oregon Consumer Privacy Act 2024	X	X	X	P	X	X	X	X~	
Texas Data Privacy and Security Act 2024	X	X	X	P	X	X	X	X~	
Utah Consumer Privacy Act 2023	X		X	P	X	X			
Virginia Consumer Data Protection Act 2023	X	X	X	P	X	X	X	X~	

Table key:

X – The right or obligation exists

S – The right to opt out of processing of sensitive data

P – The right to opt out of processing for profiling or targeted advertising purposes

X~ - The right to opt out of certain automated decision making.

L – The right of action against businesses for certain violations

Each of the rights are outlined below:

- The right to access – This right allows a consumer to access personal data / personal information from a data controller the information or categories of information collected about a consumer, the information or categories shared with third parties.
- The right to correct – This right allows a consumer to request that incorrect or outdated personal data / personal information be corrected but not deleted.
- The right to delete – This right allows a consumer to request deletion of personal data / personal information under certain circumstances.
- The right to opt out of certain processing – This right allows a consumer to restrict a business’s ability to process information about them.
- The right to portability – This right allows a consumer to request personal data / personal information about them to be disclosed in a common file format.
- The right to opt out of sales – This right allows consumers to opt out of the sale of personal data / personal information about the consumer to third parties.
- The right to opt in for sensitive data processing – This right allows consumers to opt in before a business can process their sensitive data.
- The right against automated decision making – This right prohibits a business from making decisions about a consumer based solely on automated decision making with no human input.
- The private right of action – This right currently only applies in California but gives consumers the right to seek civil damages from a business for violations of Californian law.

*Note – Individuals have these rights, but they may only be exercised in certain circumstances.

To submit a request to exercise any of the above rights, please contact privacyoffice@eso.com.

Complaints

The Information Commissioner's Office (ICO) is the UK supervisory for upholding information rights. If you are unsatisfied with our response to any data protection or personal information issues you raise with us, you have the right to make a complaint to the ICO. We would, however, appreciate the opportunity to deal with your concerns before you approach the ICO, so please contact us in the first instance.

If you are located in the EEA or Switzerland, you can find details of your local authority [here](#).

How to contact us

If you require any further clarification regarding this Privacy Notice, please contact: people.operations@eso.com

Office Addresses:

USA: 2803 Manor Road, Austin, TX 78722

UK - 42 Fountain Street, Belfast BT1 5EF.

Denmark - Skodsborgvej 234, Søllerød, 2850 Nærum

Czech Republic - nám. T. G. Masaryka 1931/12 - floor 3

Canada - 43 Goldthorne Ave, Toronto, ON M8Z 5S7, CA

Updated: 23 December 2024